基于GDPR的个人数据保护企业自评指标体系研究*

■ 许济沧[1] 安小米[1,2,3] 孙嘉睿[1] 吴国娇[1] 汪力[1]
[1] 中国人民大学信息资源管理学院 北京 100872 [2]数据工程与知识工程教育部重点实验室 北京 100872
[3] 中国人民大学智慧城市研究中心 北京 100872

摘要：[**目的/意义**]为解决我国企业面对欧洲《通用数据保护法》(GDPR)的涉欧个人数据管理难题，建立完善我国个人数据保护评价性指标体系，促进我国企业个人数据保护管理工作。[**方法/过程**]结合GDPR的具体条款，采用AHP层次分析法，构建一套基于GDPR适用于中国企业的个人数据保护自评指标体系。[**结果/结论**]指标体系可满足现有企业应对GDPR开展自评的基本需求。同时体系中由GDPR条款所衍生出的指标对完善《信息安全技术 个人信息安全规范》等国家标准有参考性价值。

关键词：GDPR 个人数据保护 指标体系 层次分析
分类号：G203
DOI：10.13266/j.issn.0252-3116.2018.23.014

2016年4月14日，欧洲议会投票通过了讨论4年之久的《通用数据保护法案》(General Data Protection Regulation，GDPR)[1-2]。该法案将于2018年5月25日正式生效，无需转换，作为欧盟统一的法律，保障成员国个人信息的安全。相较于《1995年个人信息保护指令》(GDPR生效后废止)，新法案以法律而非指令的形式生效，极大地避免了各国法律转换过程中尺度不一的问题[3]。同时新法还保障了个人对其信息的控制权[4]，重新分配了信息控制者、处理者之间的义务和责任，完善了信息跨境和刑事活动领域的特殊信息保护规则[5]。

GDPR不仅对欧洲个人信息保护法律体系是一次重大变革，还对我国企业涉欧数据业务产生重要影响[6]。GDPR第二条第一款规定，该法适用于完全或部分以自动方式对个人数据的处理。第三条规定，欧盟境内的数据处理者、数据控制者无论处理行为是否在境内，均受到该法约束。同时，该法适用于欧盟内的数据主体的个人数据处理，即无论数据处理者、控制者是否在欧盟境内，处理其境内个人数据，也将受到该法约束[7]。可见我国企业涉欧个人数据业务，特别是通讯、大数据等业务将受到新法的考量，而违法的代价也是巨大的。GDPR建立了层列式的法律责任制度，进一步增加了法律责任。一方面，GDPR第83条第2款规定了11项行政处罚的裁量情节，第3-6款则规定了不同类型的违法行为最高处罚上限。根据规定，违反信息跨境流动要求和未经信息主体许可的收集、处理等行为，最大处罚额可达到2 000万欧元或者当年全球收营业额的4%[8]。这一罚款额对于许多中国涉欧数据企业而言，足以导致其破产、倒闭。而现实中，许多涉事中小企业对GDPR了解甚微，更不知如何合规开展个人数据管理。

同时，GDPR自身通过了长达4年的论证，是国际个人数据保护立法的里程碑。通过人员、流程和产品控制组合实现个人数据保护的合规性，其概念体系构建独具创新性。另外，GDPR对于隐私数据的定义，对数据保护官职责的分配，对境外数据的管控也极具参考性。相比而言，国内法律、标准尚有完善空间。最后，作为通用性个人数据保护法律，GDPR留有很大解释空间，大部分条款属于通用性原则要求，非常适合采纳借鉴。而近年，我国大数据技术、机器学习技术蓬勃发展，对个人数据的收集及挖掘日益频繁，个人隐私数据安全问题凸显。我国相关部门和研究机构通过国家

* 本文系国家社会科学基金重大项目"国家数字档案资源整合与服务机制研究"(项目编号：13&ZD184)研究成果之一。
作者简介：许济沧(ORCID：0000-0003-4661-3278)，硕士研究生；安小米(ORCID：0000-0002-6283-2289)，教授，博士，博士生导师，通讯作者，E-mail：anxiaomi@ruc.edu.cn；孙嘉睿(ORCID：0000-0003-3194-922X)，硕士研究生；吴国娇(ORCID：0000 0002 0610 1932)，硕士研究生；汪力(ORCID：0000-0002-8063-0381)，硕士研究生。
收稿日期：2018-06-01 修回日期：2018-08-12 本文起止页码：113-118 本文责任编辑：徐健

指导性标准和国家推荐标准等形式对相关主体(主要数据控制及利用者为企业)进行管理规范。但相对法律形式的 GDPR,相关标准的法理性与落地实用性并不理想。如能补充 GDPR 中有益内容,同时针对我国标准给出评价性指标体系,激励并引导企业开展个人数据保护管理工作,对我国个人数据安全保障大有裨益。

基于以上两点原因,一套基于 GDPR 适用于中国企业的个人数据保护自评指标体系亟待建立。

1 国内现有研究

我国首个个人信息保护体系是由中华人民共和国工业和信息化部指导,中国软件评测中心拟定,国家标准化管理委员会归口的 GB/Z 28828 – 2012《信息安全技术、公共及商用服务信息系统个人信息保护指南》[9]及其相关指标测评体系。历经 2008 年中国软件评测中心起草《个人信息保护规范》,2010 年 5 月 11 日更名《个人信息保护指南》,2011 年 9 月 23 日,讨论修改名称为《信息安全技术、公共及商用服务信息系统个人信息保护指南》该标准最终于 2013 年 2 月 1 日起实施,其体系基本构建完成。该标准明确在个人信息处理的收集、加工、转移、删除 4 个环节中信息主体、管理者、获得者和第三方测评机构的角色与职责[10]。其最显著的特点是规定个人敏感信息在收集和利用之前,必须首先获得个人信息主体明确授权[11]。这项标准还提出了处理个人信息时应当遵循的 8 项基本原则,即目的明确、最少够用、公开告知、个人同意、质量保证、安全保障、诚信履行和责任明确。

自 2014 年始,一些学术机构也开展了企业个人信息保护指标及测评的相关研究,其中由北京大学互联网法律中心张平教授带领的团队,联合中国科学技术法学会于 2015 年 12 月发布最新版《互联网企业个人信息保护测评标准》(以下简称《标准》)[12]。并连续发布了《互联网企业个人信息保护抽样测评报告》,形成了第三方测评约束的企业个人信息保护体系[13]。《标准》以知情同意原则、合法必要原则、目的明确原则、个人参与原则、信息质量原则、安全责任原则为基本原则,制订了包括知情同意、收集、加工、使用、转移、个人参与、政策修改、安全责任、特殊领域的个人信息在内的指标体系[14]。张平教授表示,《标准》的目的与价值在于从操作层面积极推进互联网领域的个人信息保护,促进行业自律。互联网企业可以以《标准》为依据对其个人信息保护政策及实践做法进行比照,及时调整政策文本和实践做法;监管部门、第三方机构、用户等能够依据《标准》对互联网企业个人信息保护工作进行评估[15]。

我国最新的个人信息安全保护体系是由全国信息安全标准化技术委员会(SAC/TC260)提出并归口,由北京信息安全测评中心、中国电子技术标准化研究院、四川大学、北京大学、清华大学、阿里巴巴(北京)软件服务有限公司、深圳腾讯计算机系统有限公司等共同起草的 GB/T 35273 – 2017《信息安全技术 个人信息安全规范》[16]。该标准为国家鼓励采用推荐性标准,适用于“主管监管部门、第三方评估机构等组织对个人信息处理活动进行监管、管理和评估”。在此之前,国家网信办明确指出,规范“定位为我国个人信息保护工作的基础性标准文件,为制定和实施个人信息保护相关法律法规奠定基础”[17]。该标准体系特点是契合《中华人民共和国网络安全法》实施过程中企业安全义务与责任落实的要求,规范了个人信息收集的合规要求、个人信息分享的合规要求、用户控制个人信息的合规要求、企业个人信息管理制度的合规要求、阿里巴巴及腾讯隐私政策的主要内容及合规要求。同时规范明确了个人信息控制者开展个人信息处理活动时的 7 项原则包括:权责一致、目的明确、选择同意、最少够用、公开透明、确保安全、主体参与。

综上可见,我国在企业个人信息保护方面已形成至少三套标准体系,满足基本的监管、评估要求,但是,这些标准体系缺乏对应评估打分的指标体系,难以落地。另外,包括张平教授的《互联网企业个人信息保护测评标准》在内的体系大多追求全面性,缺乏针对性,加重了企业的业务负担和经济负担。

本研究结合 GDPR 的具体条文与刚生效的《信息安全技术 个人信息安全规范》国家标准原则、《信息安全技术、公共及商用服务信息系统个人信息保护指南》原则,构建了一套涵盖个人数据收集、保存、使用、传输、安全处置、约束管理阶段的企业个人数据管理评价指标体系,并通过专家问卷调查法、AHP(层次分析法)对各指标进行赋权和打分,通过实际案例应用验证了指标体系的正确性。该指标体系具有简洁、可操作、针对性强的特点,可满足现有企业应对 GDPR 开展自评的基本需求。同时,体系中由 GDPR 条文所衍生出的指标对完善《信息安全技术 个人信息安全规范》国家标准有参考性价值。

许济沧, 安小米, 孙嘉睿, 等. 基于GDPR的个人数据保护企业自评指标体系研究[J]. 图书情报工作,2018,62(23):113-118.

2 评价指标分析

本指标体系共包含三层(见图1):①第一层为目标层,即评估企业层面上保护个人隐私数据的基本情况;②第二层为原则层,包含了8项重要原则,这些原则来自对国家标准及GDPR的核心原则的融合,同时本体系按照个人数据安全保护的流程,对8项重要原则进行了划分;③第三层为指标层,包含17项实用指标,是经过对GDPR全文的梳理、概括和提炼得出,对企业评估自身与GDPR差距提供重要参考。

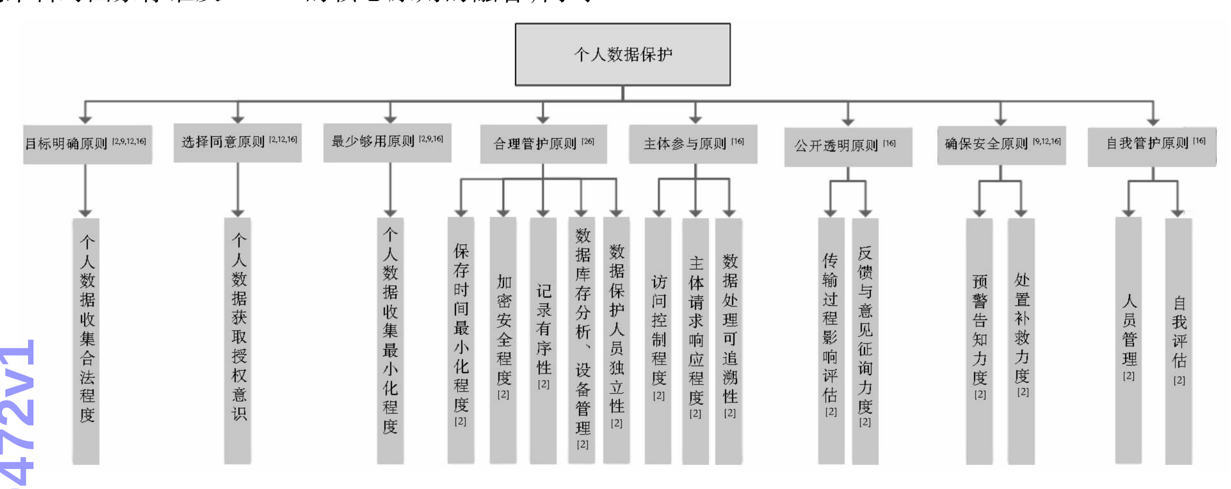


图1 GDPR企业个人信息保护指标分层体系

本指标体系中的原则层,从GDPR与国内三套标准的原则中筛选合并,遵循数据主体相关、数据过程相关的筛选合并准则,包含以下原则:目的明确原则、选择同意原则、最少够用原则、合理管护原则、主体参与原则、公开透明原则、确保安全原则、自我约束原则。其中,目的明确原则、选择同意原则与最少够用原则是GDPR提及的基本原则。合理管护原则、主体参与原则、公开透明原则、确保安全原则与自我约束原则采自我国推荐性国家标准《信息安全技术 个人信息安全规范》即"中国的GDPR"。目的明确原则是指在个人数据收集阶段,对个人数据的采集要确实出于业务需要而开展。选择同意原则要求对个人数据的收集应该采用显性书面申明的形式,任何形式刻意隐藏导致无意识签署个人信息获取协议的行为均是违法和无效的。最少够用原则要求采集的频率和数量都要满足最大限度的少量原则,并且与实现业务功能直接相关。合理管护原则是通过对GDPR与国家标准中个人数据保存阶段重要环节的概括得出的原则,包含了保存时间最小化程度、加密安全程度、记录有序性、数据库存分析、设备管理、数据保护人员独立性等指标,旨在测评企业在应对GDPR上,个人数据保存过程中的匿名性、安全性和有序性。主体参与原则由个人数据使用阶段的访问控制、主体请求、活动追溯等指标要求构成,是指在个人数据的使用过程中企业应给予信息的拥有者修改、删除等数据权利,并对个人数据使用过程中的活动进行有效记录,合理分配访问权限给予数据拥有者合理的数据访问权利、副本获取权利。公开透明原则指在个人数据传输阶段,对跨国转移等行为的传输过程影响要公开进行评估,取得同意之后才可开展相应的传输活动。此外,需要对反馈与意见进行征询,建立监督与投诉程序。确保安全原则是指个人数据安全处置阶段,企业需具备一定的预警告知机制,能够通知数据监管部门与数据拥有者,尽可能降低数据安全事件发生时的损失。同时在此过程中,企业还应当具备一定的处置补救措施或是应急预案。自我约束原则是指在企业全过程管理过程中应有效管理企业集团或从事联合经济活动的企业集团及其成员的结构和联系方式,对人员形成控制。同时应该根据企业规模设立数据保护官,对数据全过程所涉及的逻辑程序以及对数据主体开展梳理、评估。

指标层均筛选自GDPR原文,覆盖数据管理的各阶段,具有针对性强、法理逻辑合理等特点,对原则层有更具体衡量,表1附有各指标的涵义与解释。

3 评价指标权重

本指标体系通过个人数据管理过程划分各指标应用的阶段,因此指标之间相互独立,适合使用层次分析法(AHP)进行权重计算。AHP是指标体系赋权的一种重要的半定性与半定量结合的方法。通常通过专家问卷采集两两指标之间的重要程度信息, 通过计算各

表 1 GDPR 企业个人信息保护评价指标体系

数据管理阶段	原则	指标	解释说明
个人数据收集阶段	目的明确原则[2,9,12,16]	个人数据收集合法程度	不得诱骗、欺诈、强迫提供个人数据,不得违法收集个人数据。GDPR 第九条规定:对揭示种族或民族出身,政治观点、宗教或哲学信仰,工会成员的个人数据,以及以唯一识别自然人为目的的基因数据、生物特征数据,健康、自然人的性生活或性取向的数据的处理应当被禁止
	选择同意原则[2,12,16]	个人数据获取授权意识	直接或间接对个人数据的后阶段使用获权,应采用显性书面声明方式,模板见 GDPR 附表
	最少够用原则[2,9,16]	个人数据收集最小化程度	采集个人数据的频率、数量满足最大限度的少量原则,并且与实现业务功能直接关联
个人数据保存阶段	合理管护原则[16]	保存时间最小化程度	–
		加密安全程度	个人身份识别数据删除或加密、数据匿名化程度
		记录有序性	GDPR 第二十八条规定:企业应保持井然有序的记录
		数据库存分析、设备管理	要了解数据的存储位置、访问者以及已经存储了多长时间
		数据保护人员独立性	GDPR 第三十八条第三款规定:控制者和处理者应当确保对数据保护人员不下达任何指令,他们不能因为执行任务的原因而被解雇或者受到刑事处罚。数据保护人员直接向最高管理者报告工作。
个人数据使用阶段	主体参与原则[16]	访问控制程度	–
		主体请求响应程度	GDPR 第十三条规定:个人数据更正、删除、账户注销、获取副本、申诉数据系统自动决策
		数据处理可追溯性	GDPR 第三十条规定:每一位控制者,应当依其职责保持处理活动的记录。记录应当包括以下所有数据:(a)控制者、控制者代理人和数据保护员的姓名和联系数据;(b)处理的目的;(c)数据主体的类别和个人数据的分类的描述;(d)个人数据已经或将要被公开的收件人的类别,包括在其他国家或国际组织的收件人
个人数据传输阶段	公开透明原则[16]	传输过程影响评估	需规定向不受具有约束力的公司规则约束的机构转移的要求;数据传输所涉第三国的身份;过程中受影响的数据主体类型
		反馈与意见征询力度	建立监督、投诉程序
个人数据安全处置阶段	确保安全原则[9,12,16]	预警告知力度	–
		处置补救力度	GDPR 第三十条第一款规定:在个人数据泄露的情况下,控制者不能不当延误,而且至少应当在知道之时起 72 小时以内,根据第五十五条向监管机构进行通知。GDPR 第三十三条第三款规定:(a)对于所泄露的个人数据的性质进行描述,包括相关数据主体以及数据记录的种类和大致数量;(b)和数据保护局或者是其他获取更多数据的联系点交流名称和联系方式;(c)描述个人数据泄露的可能情况;(d)重视个人数据泄露问题,描述控制者采取的或者计划采取的措施,包括在适当情况下能够减轻可能的负面影响的措施。
企业整体约束管理阶段	自我约束原则[16]	人员管理	有效管理企业集团或从事联合经济活动的企业集团及其成员的结构和联系方式
		自我评估	GDPR 规定:250 人以上企业需要数据保护官。GDPR 第二十二条第一款以及第四款提到的分析过程所涉及的逻辑程序以及对数据主体的处理过程的重要意义和设想结果

指标比较得分的几何平均值,归一化后得出各指标的权重,经矩阵一致性检验通过之后,确定为最终权值。本研究于 2018 年 6 月向信息资源管理领域、大数据领域的 6 位专家小范围投放了指标体系的调查问卷,通过认真计算得出各原则和指标的权值,见表 2。

各原则的权重如 Wi 列所示,矩阵一致性检验 CR 值为 0.014 1 远小于 0.1,赋权结果有效。通过原则层对目标层的赋权分析,发现合理管护原则、确保安全原则、主体参与原则、选择同意原则权重较高,是专家认为应该重点关注的企业个人数据管理原则。

通过各指标相对原则层各原则的单层排序和一致性检验计算(篇幅有限省略),进行层次总排序的计算,得出最终各指标的权重。计算过程见表 3。

层次总排序一致性检验过程中 CR 为 0.038 6,小于 0.1,矩阵一致性良好,表中总排序一列结果即为最终各指标赋权排序结果。其中预警告知力度、个人数据获取授权意识、访问控制程度是权重前三的指标。

4 结语

本研究通过构建企业个人数据管理指标体系,明确了目前 GDPR 中的一些重要原则和指标,对相关国家标准形成有益补充。如合理管护原则、主体参与原

表 2　原则层对于目标层的判断矩阵及单排序和一致性检验表

个人数据保护	目的明确原则	选择同意原则	最少够用原则	合理管护原则	主体参与原则	公开透明原则	确保安全原则	自我约束原则	按行相乘	开 n 次方	权重 Wi	Awi	Awi/Wi	CI = (λ - n)/(n - 1)	CR = CI/RI
目的明确原则	1	1/2	1	1/4	1/3	1/2	1/3	1/2	0.003 5	0.492 7	0.051 1	0.420 1	8.212 6		
选择同意原则	2	1	5	1/2	1	2	1/2	1	5.000 0	1.222 8	0.126 9	1.037 6	8.173 8		
最少够用原则	1	1/5	1	1/9	1/6	1/3	1/7	1/4	0.000 0	0.285 5	0.029 6	0.243 3	8.2101		
合理管护原则	4	2	9	1	2	3	1	2	864.000 0	2.328 4	0.241 7	1.958 3	8.101 7		
主体参与原则	3	1	6	1/2	1	2	1	2	36.000 0	1.565 1	0.162 5	1.320 7	8.128 8		
公开透明原则	2	1/2	3	1/3	1/2	1	1/2	1	0.250 0	0.840 9	0.087 3	0.706 1	8.088 4		
确保安全原则	3	2	7	1	1	2	1	2	168.000 0	1.897 4	0.197 0	1.598 2	8.113 5		
自我约束原则	2	1	4	1/2	1/2	1	1/2	1	1.000 0	1.000 0	0.103 8	0.839 5	8.086 4		
										9.632 8			8.139 4	0.019 9	0.014 1

表 3　层次总排序计算表

准则层 ai	目的明确原则	选择同意原则	最少够用原则	合理管护原则	主体参与原则	公开透明原则	确保安全原则	自我约束原则	总排序
指标层 bin	0.051 1	0.126 9	0.029 6	0.241 7	0.162 5	0.087 3	0.197 0	0.103 8	Σai * bin
预警告知力度	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.833 3	0.000 0	0.164 1
个人数据获取授权意识	0.000 0	1.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.126 9
访问控制程度	0.000 0	0.000 0	0.000 0	0.000 0	0.658 6	0.000 0	0.000 0	0.000 0	0.107 0
记录有序性	0.000 0	0.000 0	0.000 0	0.425 7	0.000 0	0.000 0	0.000 0	0.000 0	0.102 9
人员管理	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.833 3	0.086 5
传输过程影响评估	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.833 3	0.000 0	0.000 0	0.072 7
数据库存分析、设备管理	0.000 0	0.000 0	0.000 0	0.275 9	0.000 0	0.000 0	0.000 0	0.000 0	0.066 7
个人数据收集合法程度	1.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.051 1
加密安全程度	0.000 0	0.000 0	0.000 0	0.175 5	0.000 0	0.000 0	0.000 0	0.000 0	0.042 4
处置补救力度	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.166 7	0.000 0	0.032 8
数据处理可追溯性	0.000 0	0.000 0	0.000 0	0.000 0	0.185 2	0.000 0	0.000 0	0.000 0	0.030 1
个人数据收集最小化程度	0.000 0	0.000 0	1.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.029 6
主体请求响应程度	0.000 0	0.000 0	0.000 0	0.000 0	0.156 2	0.000 0	0.000 0	0.000 0	0.025 4
保存时间最小化程度	0.000 0	0.000 0	0.000 0	0.085 0	0.000 0	0.000 0	0.000 0	0.000 0	0.020 5
自我评估	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.166 7	0.017 3
反馈与意见征询力度	0.000 0	0.000 0	0.000 0	0.000 0	0.000 0	0.166 7	0.000 0	0.000 0	0.014 5
数据保护人员独立性	0.000 0	0.000 0	0.000 0	0.038 0	0.000 0	0.000 0	0.000 0	0.000 0	0.009 2

则是国家标准中还没能高度提炼和完整描述的重要原则，预警告知力度、访问控制程度等指标也对完善国标具有建设性参考价值。同时，该指标体系在保证相对完整满足国家标准原则的条件下，针对 GDPR 提出了针对性指标，对有涉欧个人数据业务的企业自评，有较大帮助。未来在大规模调研后，将进一步验证该指标体系的准确性与实际效能。此外，还将“以评代促”推进个人数据保护规范管理工作，验收指标体系社会效能，进一步深化相关研究。

参考文献：

[1] 桂畅旎. 欧盟《通用数据保护法案》的影响与对策[J]. 中国信息安全,2017(7):90 - 93.

[2] EU Congress. General Data Protection Regulation (GDPR) [EB/OL]. [2018 - 04 - 14]. https://gdpr-info.eu/.

[3] 办公自动化编辑部. 应对 GDPR[J]. 办公自动化,2017,22(16):17.

[4] 王进. 论个人信息保护中知情同意原则之完善——以欧盟《一般数据保护条例》为例[J]. 广西政法管理干部学院学报,2018,33(1):59 - 67.

[5] 刘云. 欧洲个人信息保护法的发展历程及其改革创新[J]. 暨南学报(哲学社会科学版),2017,39(2):72 - 84.

[6] 张建文,张哲. 个人信息保护法域外效力研究——以欧盟《一般数据保护条例》为视角[J]. 重庆邮电大学学报(社会科学版),2017,29(2):36 - 43.

[7] 何治乐,黄道丽. 欧盟《一般数据保护条例》的出台背景及影响[J]. 信息安全与通信保密,2014(10):72 - 75.

[8] 彭星. 欧盟《一般数据保护条例》浅析及对大数据时代下我国征信监管的启示[J]. 武汉金融,2016(9):42 - 45.

[9] 全国信息安全标准化技术委员会. GB/Z 28828 - 2012, 信息安

全技术 公共及商用服务信息系统个人信息保护指南[S]. 北京:中国标准出版社,2013.
[10] 黄子河. 个人信息安全国家标准蓄势待发[J]. 中国经济和信息化,2012(7):90-91.
[11] 人民网. 我国首个个人信息保护国家标准2月1日起实施[EB/OL]. [2018-03-21]. http://politics. people. com. cn/n/2013/0121/c1027-20274730. html.
[12] 北京大学互联网法律中心,中国科学技术法学会. 互联网企业个人信息保护测评标准[J]. 网络法律评论,2015,17(1):3-9.
[13] 北京大学互联网法律中心,中国科学技术法学会. 互联网企业个人信息保护抽样测评报告(2017)[J]. 网络法律评论,2016,(1):232-240.
[14] 张哲. 探微与启示:欧盟个人数据保护法上的数据可携权研究[J]. 广西政法管理干部学院学报,2016,31(6):43-48.
[15] 编辑部.《互联网企业个人信息保护测评标准》发布[J]. 信息网络安全,2014(4):98.
[16] 全国信息安全标准化技术委员会. GB/T 35273-2017, 信息安全技术 个人信息安全规范[EB/OL]. [2018-10-08]. http://c. gb688. cn/bzgk/gb/showGb? type = online&hcno = 4FFAA51D63BA21B9EE40C51DD3CC40BE.
[17] 李晓琳,黄春林. 网络经济时代中国企业面临的挑战及对策[J]. 中国管理信息化,2009,12(17):98-100.

作者贡献说明:
许济沧:负责研究思路设计、指标设计、指标测评等内容;
安小米:负责研究方法的指导;
孙嘉睿:负责文献综述撰写;
吴国娇:负责相关资料的收集;
汪力:修改意见反馈与责任校对。

Research on Self-evaluation Index System of Personal Data Protection Based on GDPR

Xu Jicang[1] An Xiaomi[1,2,3] Sun Jiarui[1] Wu Guojiao[1] Wang Li[1]
[1] School of Information Resource Management School, Renmin University of China, Beijing 100872
[2] Key Laboratory of Data Engineering and Knowledge Engineering, Ministry of Education, Beijing 100872
[3] Smart City Research Center, Renmin University of China, Beijing 100872

Abstract: [**Purpose/significance**] This paper aims to solve the problem of China's enterprises facing the European General Data Protection Regulation (GDPR) related European personal data management problems and to establish and improve China's personal data protection evaluation index system, promoting the management of corporate personal data protection in China. [**Method/process**] Based on the specific terms of GDPR, this paper uses AHP analytic hierarchy process to construct a self-evaluation index system for personal data protection based on GDPR for Chinese enterprises. [**Result/conclusion**] The index system can meet the basic needs of existing enterprises to carry out self-evaluation of GDPR. At the same time, the indicators derived from the GDPR clause in the system have reference value for improving national standards such as Information Security Technology Personal Information Security Regulations.

Keywords: GDPR personal data protection index system AHP analysis

《专业智库研究》书讯

上海社会科学院信息研究所研究员王世伟所著的《专业智库研究》一书,2018年10月由上海社会科学院出版社正式出版。作者自2010年8月调入上海社会科学院信息研究所从事管理和研究工作后,先后结合国家和上海的战略发展与图情公共政策,组织开展了多项国家重大、重点课题研究和国家高端智库课题研究,承担了上海市社会科学创新研究基地、上海市人民政府决策咨询研究基地领军人物工作室的智库研究工作,组织编纂出版了一批研究著作和辞典,撰写了一批研究论文,就国家和地方的战略发展和公共政策提出了一批决策咨询建议,从而对专业智库问题有了深入的认知。本书汇集了作者8年来的研究心得,其中"基础理论篇"主要是关于智库的概念、类型、功能等的理论探讨;"图情智库篇"主要是关于图书馆和情报事业发展的战略问题和公共政策的研究;"决策咨询篇"主要是对国家和上海市发展进行的一些调研和决策建议。

书名:《专业智库研究》
作者:王世伟
出版社:上海社会科学院出版社
ISBN:978-7-5520-1007-7/C·173
定价:58元